GENERAL SUPPORT CENTER - EUROPE

OPERATIONS SECURITY (OPSEC)

"THE BEST SUPPORTIN G THE BEST."

GENERAL SUPPORT CENTER – EUROPE

As a valued member of the GENERAL SUPPORT CENTER-EUROPE,
you are a vital player in our success.

GENERAL SUPPORT CENTER – EUROPE

- You also play a crucial role in ensuring your family's security just by what you know of our day-to-day operations.

- You can protect your loved ones by protecting the information that you know.

Your efforts are known as Operations Security or OPSEC.

GENERAL SUPPORT CENTER – EUROPE

THE FIVE-STEP OPSEC PROCESS

1. To identify (and continuously update) both critical information and indicators of critical information.
2. To analyze the threat to critical information.
3. To determine **OPSEC** vulnerabilities of critical information or indicators that adversaries can use.
4. To analyze and assess with the commander what level of risk can be tolerated.
5. For the commander to select and implement appropriate **OPSEC** measures that eliminate or reduce risk to an acceptable, operational level

GENERAL SUPPORT CENTER – EUROPE

The **OPSEC** process is a risk management tool which enables commanders to view an operation or activity from the enemy's perspective .

The main feature of this approach is to look at our own methods and activities from the enemy's viewpoint by putting ourselves in an enemy's shoes and asking these questions:

- What information do I need to know to damage or disrupt their intentions and actions?
- What are their vulnerabilities or weaknesses?
- What information can I get that I need?

GENERAL SUPPORT CENTER – EUROPE

WHAT IS "CRITICAL INFORMATION"?

Critical information is information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations that an enemy needs in order to gain a military, political, diplomatic, or technological advantage.

GENERAL SUPPORT CENTER – EUROPE

RELEASING CRITICAL INFORMATION

If released to an enemy prematurely, critical information

may:

- Prevent or hold up mission accomplishment
- Reduce mission effectiveness
- Cause an unacceptable loss of lives and/or damage to our resources.

GENERAL SUPPORT CENTER – EUROPE

WHAT DOES "CRITICAL INFORMATION" INVOLVE?

- Critical information usually involves only a few main items of information about our **activities, intentions, operations, etc.**
- Enemies who get this information could drastically degrade or destroy our mission effectiveness.
- Critical information may also be derived from bits and pieces of related information (indicators) that are almost always available under normal circumstances.

GENERAL SUPPORT CENTER – EUROPE

EXAMPLES OF OPERATIONS INDICATORS

- Visits of VIPs associated with a particular activity, technology, or project
- Abrupt changes or cancellations of schedules
- Delivery of specialized equipment
- Specialized training
- Increased telephone calls, conferences, and longer working hours (including weekends)
- Rehearsals of operations
- Unusual or increased trips and conferences by senior officials

GENERAL SUPPORT CENTER – EUROPE

EXAMPLES OF COMMUNICATIONS INDICATORS

- Specialized and unique communications equipr
- Increased power sources
- Increases and decreases in communications tra
- Call signs
- Transmitter or cable locations

GENERAL SUPPORT CENTER – EUROPE

EXAMPLES OF ADMINISTRATIVE INDICATORS

- Schedule changes
- Military or civilian TDY orders
- Distinctive emblems, logos, and other markings on personnel, equipment, vehicles and supplies
- Transportation arrangements
- Orders, flight arrangements, and duty rosters
- Leave cancellations

GENERAL SUPPORT CENTER – EUROPE

EXAMPLES OF LOGISTICS and MAINTENANCE SUPPORT INDICATORS

- Unique sized and shaped boxes, tanks, and other containers
- Pre-positioned equipment
- Technical representatives
- Maintenance activity
- Unique or special commercial services

THREAT ANALYSIS

- OPSEC planners and commanders must use current threat information to develop appropriate OPSEC measures.
- An OPSEC threat analysis includes identifying:
  - Enemies
  - Their capabilities,
  - Their limitations
  - Their intentions to collect, analyze, and use critical information and OPSEC indicators against us.

THREAT ANALYSIS

- This analysis must be specific and tailored to the particular

operation, test, project, geographic region, facility, etc.

- Each applicable category or method must be analyzed

separately.

VULNERABILITIES

- Vulnerabilities are weaknesses that make it easy for an enemy to obtain and use critical information either from the source of information or from an indicator of that source.

- Therefore, vulnerabilities must be either
  - denied or
  - pro-actively controlled.

OPSEC VULNERABILITY

Two conditions must be present for an *OPSEC VULNERABILITY* to exist:

- A weakness that could reveal critical information,
- An enemy who has both the intent *and* the capability to exploit that weakness (a threat).

Once identified, these conditions can normally be controlled and can eliminate or reduce the OPSEC vulnerability.

OPSEC
COST EFFECTIVENESS?

- At times, it may not be cost-effective or even possible to change the source of an OPSEC indicator.
- In that case, it may be necessary to take a pro-active approach by attempting to disrupt or confuse the enemy's ability to collect and/or accurately interpret the information.
- When OPSEC indicators cannot be changed, OPSEC measures should be considered as a means to ***control*** the adversary and their comprehension or use of our information.

OPSEC MEASURES

- OPSEC measures should:
  - Be *consistent* with operational mission needs.
  - *Deny* (by controlling) critical information, OPSEC indicators, and the sources of such information.
  - *Degrade* the effectiveness of enemy decisions.

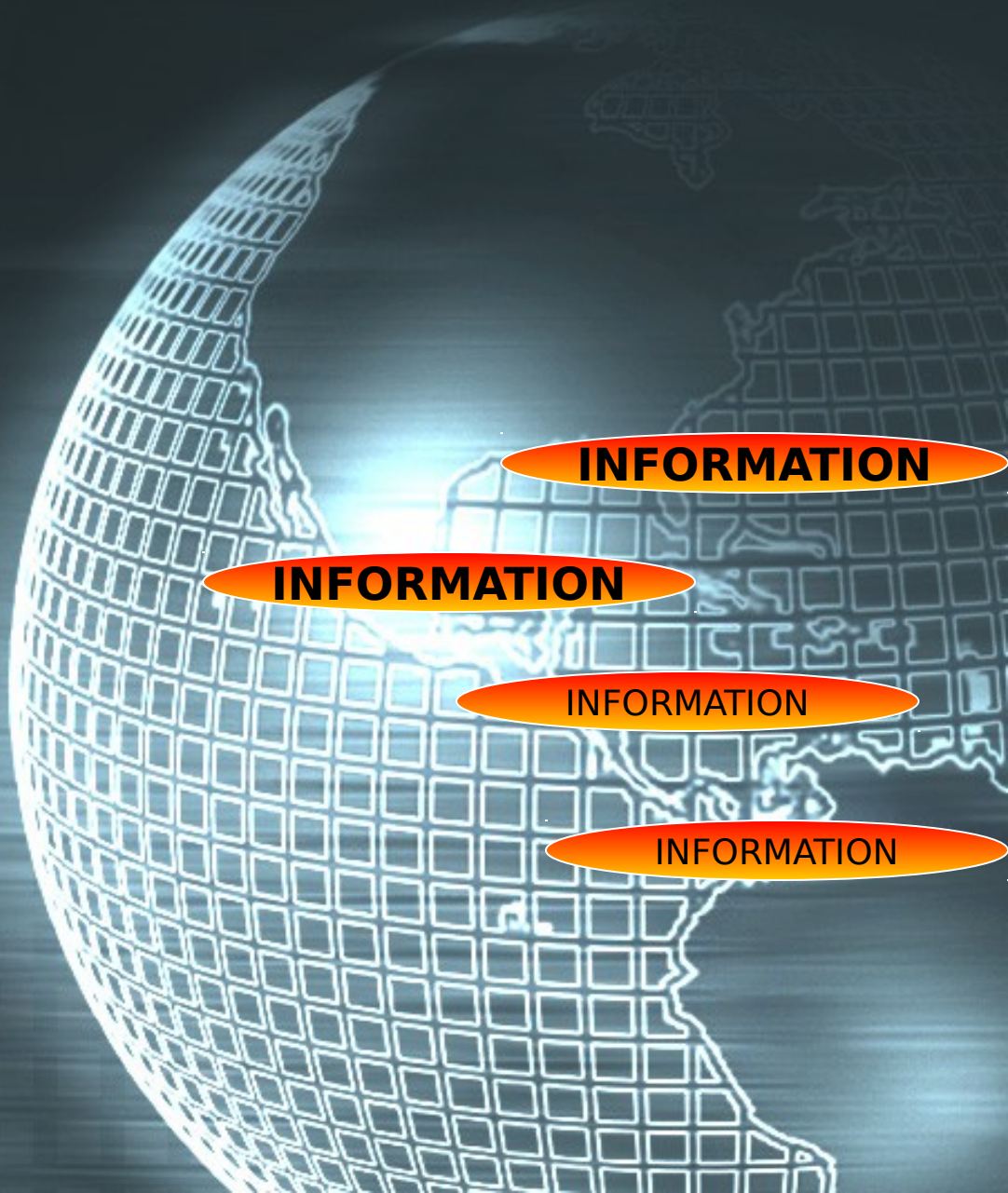
OPSEC:

is using

RISK MANAGEMENT

to protect
our information…

… ***before*** ***it gets away!***



GENERAL SUPPORT CENTER - EUROPE

OPERATIONS SECURITY (OPSEC)

"THE BEST SUPPORTIN G THE BEST."